Sicurezza su Internet

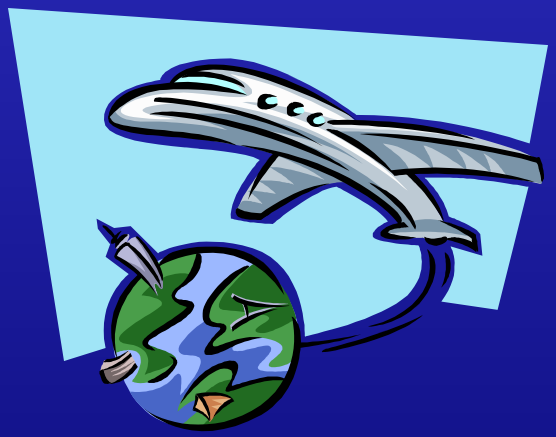
Tipi di attacchi e contromisure

Crittografia

Ph.D. Carlo Nobile

Introduzione

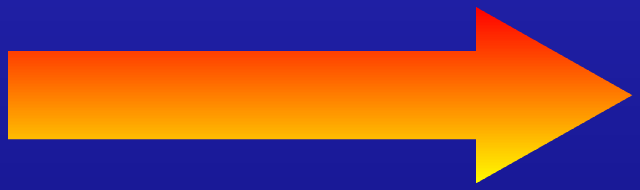
- L'informazione è un bene prezioso e deve
  - Essere custodito
  - Protetto
- I sistemi informativi sono
  - Vulnerabili
  - Esposti agli attacchi
- Problema sempre più reale
  - Diffusione dell'informatica per la raccolta ed elaborazione dei dati
  - L'espansione sempre crescente di Internet



Sicurezza su Internet

- Espansione di Internet

e la Diffusione delle reti locali – aziendali



alla circolazione e allo spostamento in rete di dati importanti quali:

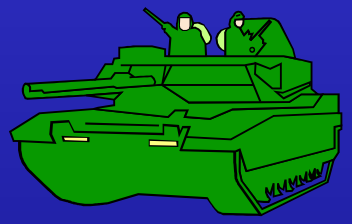
- Transazioni economiche
- Segreti industriali

Sicurezza

- Non solo in azienda …

- Ma anche sui calcolatori personali
  - Nootebook
  - Home computer (conti personali, codici di carte di credito)

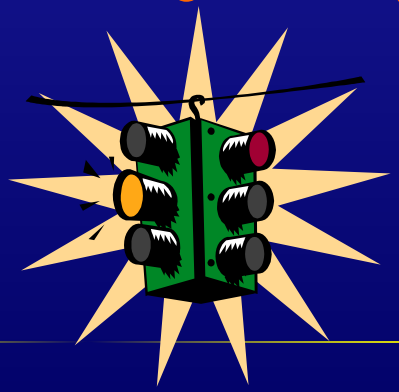
Infowarfare e cybernetic warfare



- Infowarfare
  - Termine coniato in ambito militare
  - “Serie di attività finalizzate a danneggiare il patrimonio informativo del ‘nemico’
    - Conoscenze
    - Credibilità
    - Immagine

Infowarfare e cybernetic warfare

- Cybernetic warfare
  - Insieme di azioni atte a tutelare il patrimonio informativo
    - Tecnologie impiegate (firewall, anti-intrusione, antivirus …)
    - Politiche di sicurezza interne (gestione accessi – responsabilità)
    - Educazione degli utenti (conservazione password …)



Origini Problema

- Internet nasce come sistema “aperto”
- Dopo l’avvento del Web primi tentativi di abuso su larga scala
- Anni ’80 nascita virus informatici predecessori dei *malicious coding*
- 1991 (Guerra del Golfo) gli USA attaccano e infettano la rete militare irachena
- 1992-1997 sviluppo molteplici ‘tecniche’
- 1998 Aprile il Dod degli USA annuncia di aver subito in una settimana 250.000 attacchi

Origini Problema

- Primo auditing su larga scala (1998) su commissione DoD
- Nello stesso anno l'FBI stima i possibili danni dai 100 ai 300 miliardi di dollari
- 1999 Amministrazione Clinton autorizza investimento 1,5 miliardi di dollari

Soluzione ?

- Non e' possibile trovare una soluzione esaminando il problema a compartimenti stagni
- La soluzione è "Multilivello"
  - più componenti che interagiscono
  - molto importante il fattore umano
- Inoltre ad attacchi distribuiti si devono contrapporre difese distribuite

Tre Leggi

- Mai dire mai:
  - non esiste una metodica sicura e inattaccabile definitivamente
  - Ciò che appare impossibile oggi, domani sarà realizzato
- La sicurezza totale non esiste

  (postulato)
- Non si possono risolvere i problemi di sicurezza con il solo software

  (legge di Ranum)

Beni da proteggere

- Il primo elenco evidenzia tre categorie
  - Hardware
  - Software
  - Dati
- Non meno importanti
  - Supporti di memorizzazione (software e dati)
  - Reti (scambio dati)
  - Accesso (possibilità utilizzo bene)
  - Individui chiave (amministratore sistema, operatore specializzato)

Sicurezza Informatica: Obiettivo

Garantire un adeguato grado di protezione dei *beni*, mediante l'attuazione di un progetto di sicurezza globale che, tenendo conto dei vari aspetti del problema, raggiunga un livello di protezione, organizzativo ed informatico che possa essere monitorato nel tempo.

Per realizzare ciò bisogna definire una politica di sicurezza in modo che il *bene* mantenga nel tempo le sue proprietà di disponibilità, integrità e sicurezza

Terminologia

- Abusi Tecnologici.
  - Insieme di azioni consistenti in un utilizzo distorto di una tecnologia ideata e creata per fini positivi.
- Attacker o Malicious Hacker.
  - Chi si occupa di violare i Sistemi informativi con l'intento di danneggiarli.
- Hacker
  - Idealista: viola i sistemi a scopo di "ricerca"
- Cracker
  - Viola i sistemi per fare danni

Terminologia

- Auditing Distribuito
  - Operazioni atte a verificare lo “stato di salute” di un sistema: più tipologie di verifica
- Backtraking
  - Operazioni per la localizzazione di un computer e se possibile del suo utilizzatore (in caso di violazioni)

Terminologia

- Granularità
  - Possibilità di scindere un sistema nei minimi dettagli per una migliore analisi dei punti di interesse strategico
- Information Security
  - Processo di protezione del patrimonio informativo a rischio (cybernetic warfare)
- Matching
  - Corrispondenza dei dati: tecnica utilizzata per rilevare la presenza di virus o l'attacco al sistema

Terminologia

- Security Policy
  - Regola che realizza una linea guida precostituita: di solito decisa dal management tecnico in collaborazione con un consulente legale
- Sensitive data
  - Non i dati sensibili previsti della legge sulla privacy, ma i dati sensibili di una transazione (è anche l'indirizzo IP)
- Sistemi aperti
  - Sistemi informativi eterogenei comunicanti grazie a una serie di regole standard, ovvero con un linguaggio di "connettività" comune

Terminologia

- Target
  - Obiettivo di un attacco:
    - Singolo computer (*victim machine*)
    - Rete (più calcolatori riconducibili ad un'unica entità)

Terminologia

- Virus
  - Una porzione di codice in grado di autoriprodursi e di trasferirsi “attaccandosi” ad altre entità del computer (programmi, disk sector, file di dati, …) e di “muoversi” all’interno del calcolatore
- Worm
  - Codici indipendenti si diffondono in modo svincolato da eventuali file host
  - Possono essere multipiattaforma
- Trojan horse
  - Malware nascosti in file “innocui”, se installati permettono ad un attacker (cracker) di prendere possesso del calcolatore

Nuovi Pericoli

- Phishing
  - Invio di e-mail fraudolenta
  - Richiesta dati personali di accesso (ad esempio Carta di credito, conto bancario.
  - esempio Fineco
  - esempio Bybank

C.I.A.

- Confidentiality (Riservatezza o Confidenzialità).
  - I dati non sono accessibili e/o interpretabili da chi non ne ha diritto.
- Integrity (Integrità).
  - Non deve essere possibile alterare in alcun modo i dati utilizzati in una transazione. (contrattualistica digitale, e-commerce, e-businnes …).
- Autentication (Autenticazione).
  - L'identità delle entità coinvolte nella comunicazioni deve poter essere verificata.

Sicurezza: più Livelli

Sicurezza totale è un astrazione ⇒ l'obiettivo diventa ridurre il rischio ⇒ si deve attuare una vigilanza a più livelli ⇒ separazione tra intranet e rete pubblica (WEB) tramite Firewall e introduzione di sistemi di identificazione fisici o logici.

Oggi il problema si allarga con la diffusione (costi contenuti) di Internet a Banda Larga (tramite la tecnologia ADSL) anche tra i singoli utenti che dibentano a rischio.

Un'altra fonte di rischio sono le Reti mobili.

Attacchi e Contromisure

- Sniffing
- Connection hijacking
- Denial of service (DoS)
- Spoofing
- Buffer overflow
- Malicious code
- Hyper malware
- Defacement
- “Social engineering”

Sniffing

- Intercettazione passiva delle comunicazioni dati
- Attacker: un soggetto che ha accesso diretto a determinati segmenti di rete o sistema, che ha strumenti tecnologici idonei
- Intercettazione di password, messaggi di posta elettronica e contenuti vari
- Gli strumenti informatici si chiamano sniffer

Sniffing

- I “programmi” devono essere installati su un calcolatore presente sulla rete da attaccare $\Rightarrow$ il calcolatore deve essere precedentemente violato, compromesso
- Per difendersi e’ necessario effettuare una “detection”
- Tale operazione non è semplice, un indizio è la presenza di schede di rete poste in modalità promiscua (lettura di tutti i pacchetti che transitano sul segmento di rete)
- Interessa segmenti wired e wireless (futuro ?)

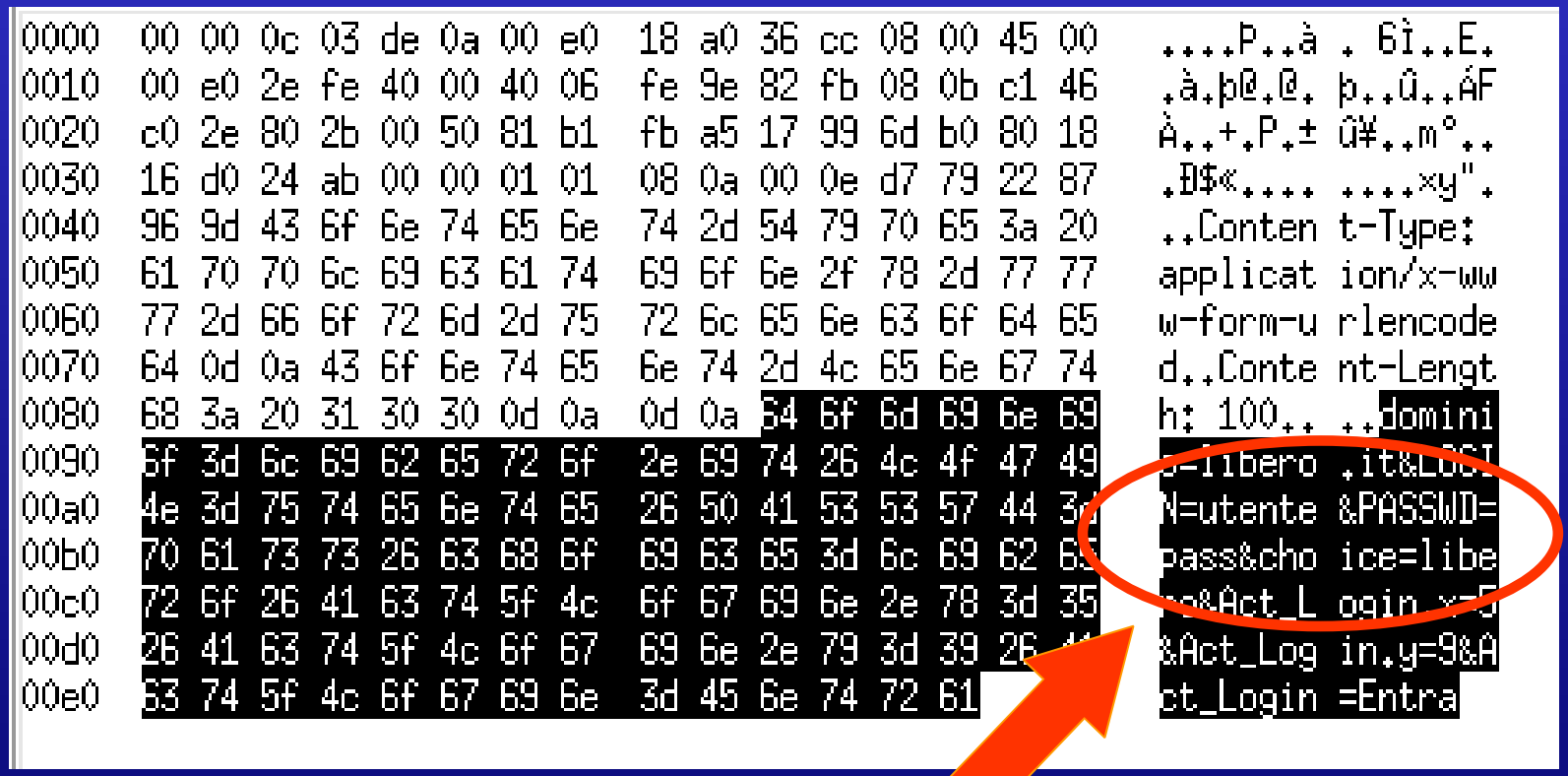
Attacchi al contenuto - Esempio di sniffing

1	0.000000	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [SYN] Seq=2175924618 Ack=0 Win=5840 Len=0
2	0.047915	wpop10.libero.it	abete.reti.dist.unige	TCP	http > 32811 [SYN, ACK] Seq=395931055 Ack=2175924619 Win=24616 Len=0
3	0.047968	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175924619 Ack=395931056 Win=5840 Len=0
4	0.048136	abete.reti.dist.unige	wpop10.libero.it	HTTP	POST /email.php HTTP/1.1
5	0.080256	wpop10.libero.it	abete.reti.dist.unige	TCP	http > 32811 [ACK] Seq=395931056 Ack=2175925157 Win=24616 Len=0
6	0.080281	abete.reti.dist.unige	wpop10.libero.it	HTTP	Continuation
7	0.223209	wpop10.libero.it	abete.reti.dist.unige	TCP	http > 32811 [ACK] Seq=395931056 Ack=2175925329 Win=24616 Len=0
8	5.503723	wpop10.libero.it	abete.reti.dist.unige	HTTP	HTTP/1.1 200 OK
9	5.503763	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175925329 Ack=395931407 Win=6432 Len=0
10	5.575033	abete.reti.dist.unige	wpop10.libero.it	HTTP	GET /error.html HTTP/1.1
11	5.595797	wpop10.libero.it	abete.reti.dist.unige	HTTP	HTTP/1.1 200 OK
12	5.595843	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175925881 Ack=395932855 Win=8688 Len=0
13	5.598326	wpop10.libero.it	abete.reti.dist.unige	HTTP	Continuation
14	5.598367	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175925881 Ack=395934303 Win=11584 Len=0
15	5.598693	wpop10.libero.it	abete.reti.dist.unige	HTTP	Continuation
16	5.598705	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175925881 Ack=395934857 Win=14480 Len=0
17	5.638893	abete.reti.dist.unige	wpop10.libero.it	HTTP	GET /old/xam_rc/template_xam/images/spacer.gif HTTP/1.1
18	5.643669	abete.reti.dist.unige	wpop10.libero.it	TCP	32812 > http [SYN] Seq=2171723094 Ack=0 Win=5840 Len=0
19	5.667858	wpop10.libero.it	abete.reti.dist.unige	HTTP	HTTP/1.1 200 OK
20	5.667898	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175926465 Ack=395935211 Win=17376 Len=0
21	5.668389	abete.reti.dist.unige	wpop10.libero.it	HTTP	GET /old/xam_rc/template_xam/images/button_err_back.gif HTTP/1.1
22	5.677580	wpop10.libero.it	abete.reti.dist.unige	TCP	http > 32812 [SYN, ACK] Seq=1219537146 Ack=2171723095 Win=24616 Len=0
23	5.677615	abete.reti.dist.unige	wpop10.libero.it	TCP	32812 > http [ACK] Seq=2171723095 Ack=1219537147 Win=5840 Len=0
24	5.677745	abete.reti.dist.unige	wpop10.libero.it	HTTP	GET /old/xam_rc/template_xam/images/header_err.gif HTTP/1.1
25	5.699033	wpop10.libero.it	abete.reti.dist.unige	HTTP	HTTP/1.1 200 OK
26	5.707494	wpop10.libero.it	abete.reti.dist.unige	TCP	http > 32812 [ACK] Seq=1219537147 Ack=2171723683 Win=24028 Len=0
27	5.741745	abete.reti.dist.unige	wpop10.libero.it	TCP	32811 > http [ACK] Seq=2175927058 Ack=395935708 Win=17376 Len=0
28	9.096682	wpop10.libero.it	abete.reti.dist.unige	HTTP	HTTP/1.1 200 OK
29	9.096723	abete.reti.dist.unige	wpop10.libero.it	TCP	32812 > http [ACK] Seq=2171723683 Ack=1219538216 Win=7483 Len=0

Attacchi al contenuto - Esempio di sniffing

```
⊟ Frame 6 (238 on wire, 238 captured)
    Arrival Time: Dec 10, 2002 13:39:46.422800000
    Time delta from previous packet: 0.000025000 seconds
    Time relative to first packet: 0.080281000 seconds
    Frame Number: 6
    Packet Length: 238 bytes
    Capture Length: 238 bytes
⊟ Ethernet II
    Destination: 00:00:0c:03:de:0a (Cisco_03:de:0a)
    Source: 00:e0:18:a0:36:cc (Asustek_a0:36:cc)
    Type: IP (0x0800)
⊟ Internet Protocol, Src Addr: abete.reti.dist.unige.it (130.251.8.11), Dst Addr: wpop10.libero.it (193.70.192.46)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 224
    Identification: 0x2efe
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xfe9e (correct)
    Source: abete.reti.dist.unige.it (130.251.8.11)
    Destination: wpop10.libero.it (193.70.192.46)
⊟ Transmission Control Protocol, Src Port: 32811 (32811), Dst Port: http (80), Seq: 2175925157, Ack: 395931056
    Source port: 32811 (32811)
    Destination port: http (80)
    Sequence number: 2175925157
    Next sequence number: 2175925329
    Acknowledgement number: 395931056
    Header length: 32 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 5840
    Checksum: 0x24ab (correct)
  ⊞ Options: (12 bytes)
⊟ Hypertext Transfer Protocol
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 100\r\n
    \r\n
    Data (100 bytes)
```

Attacchi al contenuto - Esempio di sniffing



Login: **utente**

Password: **pass**

Ph.D. Carlo Nobile

Connection Hijacking

- Riguarda le transazioni o comunque i flussi di dati point-to-point
- Non è una tecnica semplice da attuare è necessaria una certa rapidità nell'azione per impossessarsi dei dati che interessano per continuare la transazione
- L'attacker simula di essere una macchina che in realtà non è in modo da ottenere l'accesso

Contromisure a Connection Hijacking

- Adozione della Crittografia.
  - sia per gestire la cifratura dei dati scambiati;
  - sia l'autenticazione dei due poli della transazione.

Denial of Service

- Ha come scopo rendere l'obiettivo difficile o addirittura impossibile da raggiungere
- La tecnica di tale attacco prevede l'invio di un flusso consistente e continuo (flood) di dati verso l'obiettivo con il fine di rallentarlo e/o mandarlo in "crash"
- Può essere singolo o distribuito ovvero indirizzato ad un singolo calcolatore o verso una rete

Denial of Service

Si distingue tra

- DoS local based
  - Programmi che volutamente o involontariamente vanno in “crash”
- DoS network based
  - Realizzati in maniera distribuita e organizzata di solito contro obiettivi di un certo rilievo
- Bandwidth consumption
  - Inibizione della risposta del target (in gergo: riempendo il tubo)

Contromisure al Denial of Service

- Complessa: alcuni effetti si possono solo mitigare
- E' utile l'impiego di
  - firewall (filtri in ingresso e in uscita)
  - "Intrusion detection systems" per individuare la presenza di agenti (zombies) e di malicious code

Spoofing

- Non è un'intrusione in senso stretto, ma una serie di operazioni funzionali alla penetrazione di altri attacchi.
- "Spoofare" un indirizzo significa falsificarlo.
- Principalmente, o meglio inizialmente, si agisce sugli indirizzi IP, ma tale tecnica è attuata anche su altre categorie di credenziali (indirizzi di partenza della posta elettronica, numeri di telefono di partenza degli sms).
- È utilizzato per attuare tecniche DoS con il fine di mascherare le macchine attacker (anche le teste di ponte).

Contromisure Spoofing

- Crittografia rivolta ad autenticare i due poli.
- A livello IP:
  - Protocollo Ipsec;
  - Protocollo ssh (telnet sicuro).
- Per la posta elettronica:
  - Dispositivi di firma;
  - Crittografia a chiave pubblica con l'ausilio di certificati digitali.

Buffer Overflow

- Si basa sul presupposto, comune ai sistemi *nix (Linux, Unix), che alcuni programmi hanno privilegi particolari (“girano” anche come root)
- Se è presente un bug architetturale un attacker potrebbe sconvolgere le funzionalità del programma stesso prendendo possesso del calcolatore dove è installato il programma

Contromisure al Buffer Overflow

- Attenzione in fase di programmazione
- Problema costo in termini di lavoro aggiuntivo che richiede l'analisi e la verifica accurata
- Una soluzione consiste nel limitare i processi con diritti elevati assegnando ai programmi solo i diritti di cui hanno bisogno (least privilege)
- Utilizzo di strumenti di terze parti che agiscano da controllore (watchdog) intercettando possibili stringhe anomale (sintomo di prove generative di Buffer Overflow)

Malicious Code

- Macro categoria di codici che alterano e/o danneggiano (parzialmente o totalmente) il funzionamento di un sistema informatico o telematico.
- Sinonimi sono Malware e Mmc (Malicious mobile code).
- Sono compresi in questa categria alcuni codici in grado di autoriprodursi o comunque diffondersi (virus e worm).

Mass Mailing

- Malicious Code
  - Non punta, in modo prioritario, a danni logici
  - Alterazione sistemi mailer e sistemi collegati
- effetto DoS
  - Esempi:
    - BadTrans
    - Nimda
- cercano di sfruttare una particolare vulnerabilità di una piattaforma software (possibilmente molto diffusa)

Hyper-Malware - Mixed Mmc

- Insieme di più categorie malware
  - Il più in voga: worm/trojan
  - Rischio duplice
- Esempi:
  - Badtrans:
    - Possibiltà rubare password su target (possibiltà di crearsi una conoscenza da riutilizzare per altri attacchi)
  - Goner:
    - Disabilita personal firewall
    - Correlazione tra Mmc e servizio di chat come Icq

Remote Access Trojan

- Agisce sulle modalità di accesso remoto modificando il numero chiamato
  - Spese telefoniche stratosferiche
- Ad esempio i frequentatori delle newsletter di mailing list a luci rosse hanno attivato gli attach senza verificarli …

Defacement

- I “graffitari” del Web
  - Modificare o sostituire una o più pagine di un sito
  - Danni all’immagine
- Contromisure
  - Hardening
    - Azione mista di aggiornamento dei sistemi e rafforzamento della loro configurazione
    - Associata a controllo di accesso e l’uso di Intrusion Detection System

Social Engineering

- Tecnica psicologica
  - Sfrutta l'inesperienza degli utenti per mettere in essere attacchi o recare danni
    - Furto di password
    - Sulfnbk.exe (burla; fake alert per cancellarlo)
      - In realtà esistono copie di questo file contaminate dal virus magister che sono inviate via e-mail
  - Difesa principale: educazione utenti

Riassumendo: Difese da attuare

- Reattività: esempio aggiornando frequentemente il pattern degli antivirus (efficiente per fermare goner, non con badtrans che sfrutta una debolezza della piattaforma)
- Aggiornamento piattaforme di base (sistemi operativi e applicativi)
- Software antivirus a livello client e a livello gateway

Reti Wireless

- Hanno un livello aggiuntivo per la sicurezza
- 802.11 wireless lan standard
  - Wired Equivalent Privacy
    - Vuole rendere equivalente dal punto di vista fisico la trasmissione wireless con quella via cavo
  - Advanced Encryption Standard: algoritmo simmetrico che sostituisce il DES (il rilascio in concomitanza con Wep 2)

Reti Wireless

- Wireless application protocol utilizzando il livello Wtls (Wireless transport layer security) che ha il compito di
  - Garantire autenticazione
  - Integrità dei dati
  - Privacy
- Il tutto compatibilmente con le capacità di calcolo dei terminali wireless

Sicurezza nel wireless

- I problemi sono due
  - Comunicazione tra dispositivi wireless
  - Comunicazioni con siti di commercio elettronico e remote banking
    - Questi ultimi usano Ssl (Secure Socket Layer) quindi deve esserci un gateway che effettua la conversione … qui potrebbe esserci l'intercettazione anche se attualmente si tratta di un operazione non semplicissima da effettuare, ma è molto pericolosa e quindi deve essere considerata.

Malicious Code

- Attualmente sono un pericolo remoto, ma alcuni produttori hanno rilasciato soluzioni per i Personal Digital Assistant e i wap gateway
- Pki: per l'autenticazione ci si affida alle Public key infrastructure
  - Insieme di tecnologie e policy che si appoggiano alla crittografia e ai certificati digitali
    - Algoritmi a chiave pubblica
    - Problemi di complessità per il mondo wireless

Soluzioni e prospettive

- Portare il livello di sicurezza proprio delle reti cablate alle reti wireless
- La comunità tecnico-scientifica prevede una stabilizzazione della wireless security progressiva

I sistemi di protezione delle reti

- Firewall
- Reverse proxy
- Intrusion Detection System

Firewall

- Realizza uno strato di:
  - Controllo degli accessi
  - Monitoraggio della sicurezza
- Posto tra la rete interna e quella esterna
  - Protocollo base TCP-IP
- Usa le tecnologie
  - Proxy
  - Packet filtering
  - Stateful Inspection

Proxy

- Tra il programma client, residente sul computer di un utente, e un server residente su un qualsivoglia server in Internet
- Decide se i tentativi di accesso sono consentiti o meno in base ai parametri impostati

Packet Filtering

- Tecnica di analisi dei pacchetti in transito
- I pacchetti vengono filtrati in base a delle regole stabilite a priori

Stateful Inspection

- Tecnica avanzata di ispezione dei pacchetti in transito
- attualmente utilizzata da alcuni software commerciali
  - Se ben realizzata è ritenuta una delle più efficaci

Personal firewall

- Legge sulla privacy e sue integrazioni (dpr 318/99 introducono degli obblighi)
- Protezione della rete distribuita su più livelli
  - Perimetrale
  - Sulle singole postazioni
- Nasce come ultimo punto di difesa
- Gestisce i tentativi di accesso non bloccati a livello di rete e integra l'azione degli antivirus

Reverse Proxy

- Posizionato tra il firewall e la Dmz (zona demilitarizzata dove vengono posizionati i server web e simili)
- Effettua una sorta di inoltro, subordinato a un controllo di sicurezza, del traffico diretto verso una delle risorse da lui gestite
- Obiettivo: fungere da unico punto di controllo nei confronti delle transazioni provenienti dall'esterno verso determinati obiettivi a rischio

Reverse Proxy

- Si basa sul presupposto che gli attacchi avvengono a livello di applicazione
- Passano attraverso il firewall o per cattiva configurazione o perché non si effettua un controllo totale a basso livello del codice in transito
- Altro motivo il mancato hardening (rafforzamento)
- Molto costoso in termini hardware e software

Intrusion Detection System

- Funzione di auditing
  - Registrare i tentativi di attacco
  - Consente la segnalazione delle possibili violazioni in atto
- File di log
  - Bisogna proteggerli: chi effettua un accesso illegale cerca sempre di modificarli per divenire invisibile
- Processano i vari file di Log per segnalare violazioni in atto

Intrusion Detection System

- Modo di operare
  - Real-time durante l'attacco; con varie segnalazioni all'amministratore di sistema
  - Post-incidente
- Metodiche
  - Controllo delle firme degli attacchi
    - Come per gli antivirus
  - Riconoscimento anomalie
    - Comportamenti del sistema diversi da quelli standard su cui il software Ids è stato istruito

Crittografia

Ph.D. Carlo Nobile

Sommario

- Introduzione
- Cifratura a Chiave Simmetrica
- Cifratura a Chiave Pubblica
- Autenticazione
- Firma Elettronica
- Distribuzione delle Chiavi
- Protocolli

Sicurezza nelle reti

- Ci sono tre aree in cui bisogna intervenire per rendere una rete sicura
  - **Riservatezza (Confidentiality)**: il messaggio deve essere accessibile (visualizzabile o rilevabile la sua presenza) sola ad entità autorizzate.
  - **Autenticazione**: L'identità delle entità coinvolte nella comunicazioni deve poter essere verificata.
  - **Integrità (Integrity)** (ed eventuale "firma"): impedire che i dati possano essere modificati se non da autorità autorizzate (con firma: anche legate all'autore, che non ne possa disconoscere la paternità).

Sicurezza nelle reti
Attacchi

Passivi

- **Accesso al contenuto**: venire a conoscenza di informazioni riservate.
  Ad esempio lo *Sniff* (il fiutare) di pacchetti su LAN a mezzo condiviso.
- **Analisi del traffico**: senza vedere i contenuti specifici, riconoscere l'entità dei comunicanti e tipo e frequenza dei messaggi.
- Sono difficili da rilevare, quindi si devono prevenire.

Sicurezza nelle reti
Attacchi
Attivi

- **Sostituzione**: Farsi passare per un altro
  Ad esempio lo *Spoofing* (imbroglio) IP.
- **Replica**: copiare e riproporre un messaggio per ottenere effetti non autorizzati (ad esempio, un doppio versamento).
- **Alterazione**: modifica anche solo dell'ordine
- **Negazione del servizio**: inibire l'uso o la gestione di un sistema (anche dell'intera rete), ad esempio per impedire la generazione o arrivo di messaggi di allarme (SYN *Attack*).
- Possono sia essere rilevati e quindi fermati che prevenuti

Riservatezza: Cifratura

Alice

Testo in chiaro

Plaintext

P

Chiave K_a

Cifratura

$E_{ka}(P)$

Testo cifrato

Cipher Text

$C = E_{ka}(P)$

Passivo

Attivo

Trudy

Intruso

Chiave K_b

Bob

P

Decifratura

$D_{kb}(C)$

$P = D_{Kb}(E_{ka}(P))$

Cifratura a chiave Simmetrica

- E' una tecnica antica (Giulio Cesare)
- $K_A = K_B = \mathbf{K}$: una sola chiave
- Deve rispettare due requisiti per essere sicura:
  - Robustezza dell'algoritmo: anche conoscendo l'algoritmo ed avendo campioni di testo in chiaro e cifrato, l'intruso non deve essere in grado di decifrare il testo e scoprire la chiave
  - Mittente e destinatario devono poter ottenere in modo sicuro la chiave e custodirla efficacemente.

Attacchi al testo cifrato

- Attacco al testo cifrato (chipertext only): chi attacca ha a disposizione solo la conoscenza di una certa quantità di testo cifrato.
- Attacco al testo in chiaro conosciuto (known plaintext): chi attacca conosce alcuni campioni di testo in chiaro e i corrispondenti messaggi cifrati.
- Attacco al testo in chiaro scelto (chosen plaintext): chi attacca ha la possibilità di criptare il testo in chiaro desiderato.

Cifratura a chiave simmetrica

- Per scardinare un algoritmo di cifratura esistono due tecniche:
  - Criptoanalisi: che si basa sulla natura degli algoritmi, su campioni, su caratteristiche statistiche di P.
  - Forza bruta.

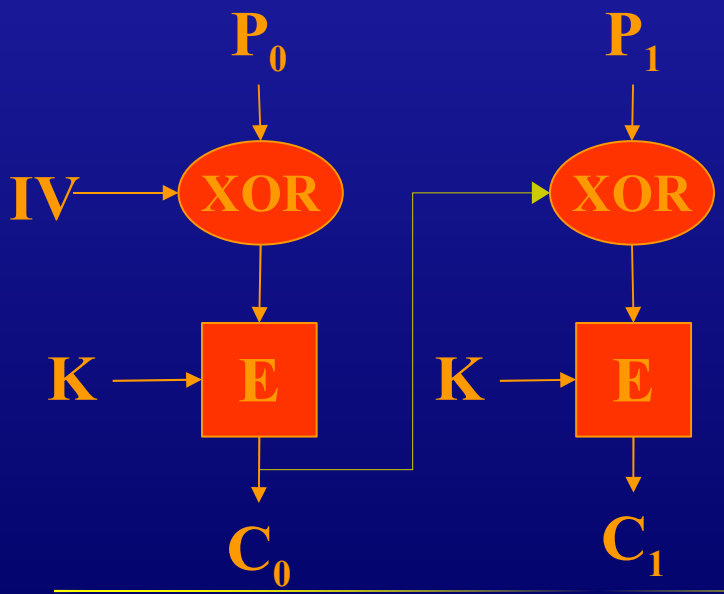
Dim. chiave	# di chiavi possibili	Tempo (1 crifr./s)	Tempo (10^6 cifr./s)
32	$2^{32} = 4{,}3 \times 10^9$	231 s = 35,8 min.	2,15 ms
56	$2^{56} = 7{,}2 \times 10^{16}$	255 s = 1142 anni	10,01 ore
128	$2^{128} = 3{,}4 \times 10^{38}$	2127s = 5,4 10^{24} anni	5,4 10^{18} anni
168	$2^{168} = 3{,}7 \times 10^{50}$	2167 s = 5,9 10^{36} anni	5,9 10^{30} anni

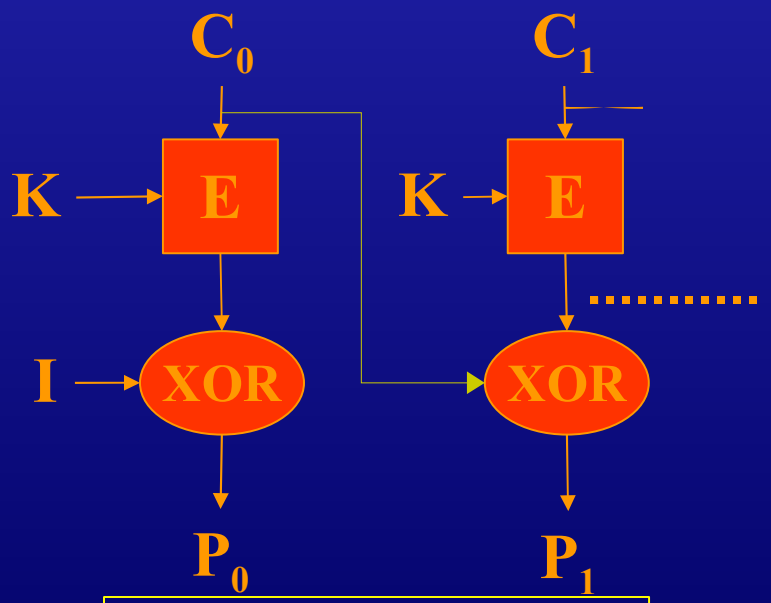
Cifratura a chiave simmetrica

- Viene in genere realizzata con una sostituzione monoalfabetica:
  - Sostituisco una “lettera” (blocco di dati) con un’altra.
- Se le lettere sono quelle dell’alfabeto (blocchi di 7 o 8 bit) ho
  - 26! possibili accoppiamenti pari a circa 10^{26}
  - Facile usare meccanismi statistici per scardinare il codice

Cifratura a chiave simmetrica

- Per rendere la tecnica più efficace
  - si usano “lettere” più grandi (ad es. n = 64 bit)e slegate dal testo, ossia si sostituisce un blocco di bit di lunghezza fissa con un altro.
  - Si concatena il risultato di una cifratura con la successiva, ossia si esegue il concatenamento di blocchi cifrati (***Cipher Block Chaining***, CBC)

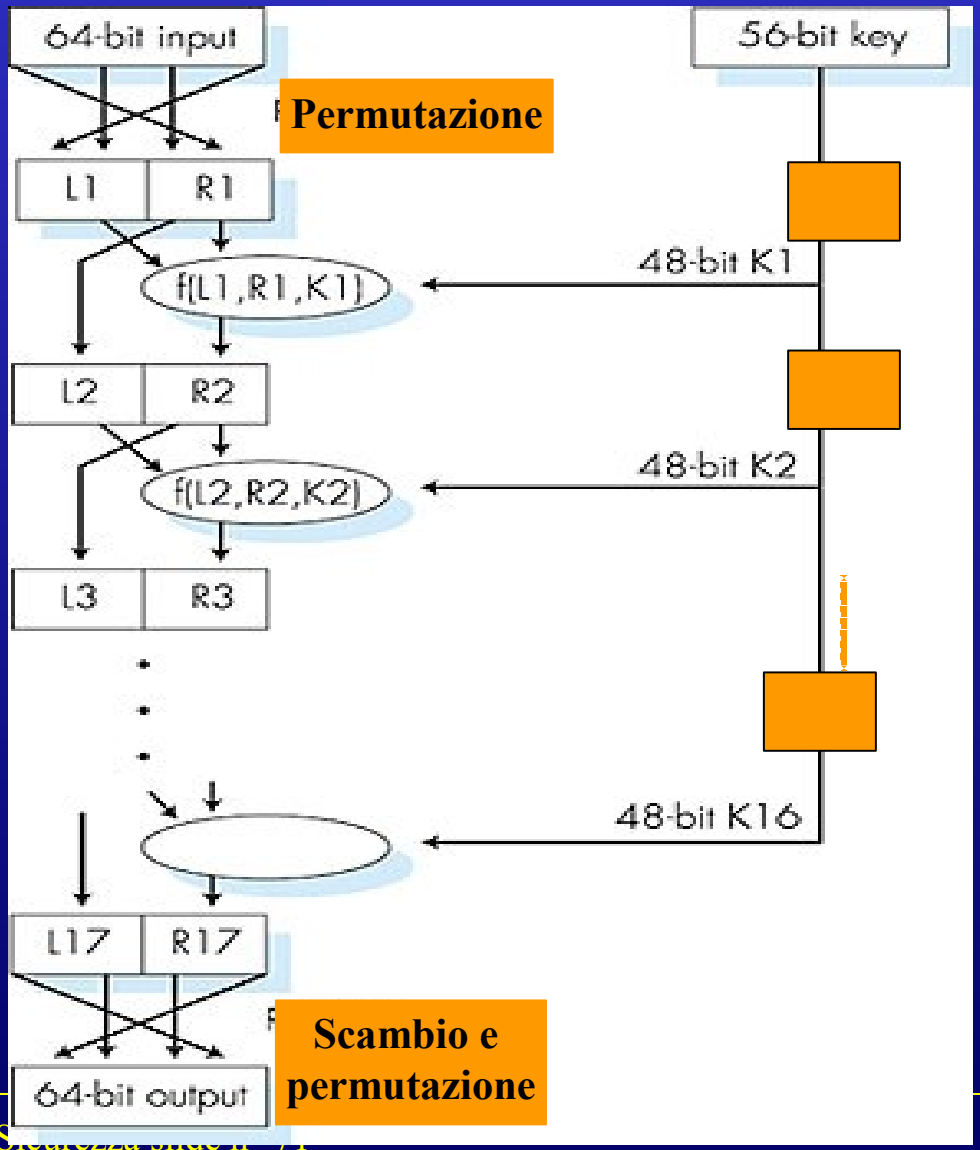




Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- Nasce nel 1977 e viene aggiornato nel 1993,
- E' stato adottato dal U. S. *National Bureau of Standard* (oggi *National Institute for Standard and Technology*, NIST)
- L'algoritmo vero e proprio si chiama *Data Encryption Algorithm* (DEA):
  - Opera su blocchi da 64 bit.
  - Usa una chiave da 56 bit.
  - Si compone di 19 stadi:
    - Una prima permutazione
    - 16 stadi parametrizzati da una variante della chiave K_i, i=1,..,16
    - Uno scambio dei 32 bit destri con i sinistri
    - Una permutazione inversa alla prima

Cifratura a chiave simmetrica
Data Encryption Standard (DES)



- In genere viene usato in unione con un concatenamento (CBC).
- La decifratura avviene con lo stesso meccanismo ma usando le chiavi in ordine inverso
- La complessità dell algoritmo risiede nella funzione f(.).

Cifratura a chiave simmetrica
Data Encryption Standard (DES)

- Per quanto concerne la robustezza, sono stati indetti tre concorsi (*challenger*) per violarlo:
  - *Challenger* I (1997): Scardinato in 4 mesi;
  - *Challenger* II (1998): Scardinato in 56 ore
  - *Challenger* II (1999) scardinato in 22 ore e 15 min. (testate 245×10^9 chiavi al sec.)
- Ad oggi, (nella sua forma con chiave a 56 bit) non è considerato molto sicuro.

Cifratura a chiave simmetrica *Triplo-DEA* (T-DEA)

- Standardizzato dall'ANSI (1985) come X 9.17 e parte del DES dal 1999
- Usa 3 chiavi da 56 bit: K_1, K_2, K_3.
- Opera come segue:

$$C = E_{K3}(D_{K2}(E_{K1}(P)))$$

- Questo significa che ha una chiave di lunghezza complessiva pari a 168 bit
- Si può cifrare e decifrare il DEA ponendo tutte le chiavi uguali
- Si può usare una chiave da 112 bit ponendo $K_1 = K_3$

Cifratura a chiave simmetrica AES

- Il National Institute of Standards and Technology (NITS), ente governativo americano, nel 1997 ha lanciato un concorso pubblico per individuare un nuovo standard di crittografia, per uso generico del governo americano
- il nome dello standard sarebbe stato AES (Advanced Encryption Standard);
- lo scopo del concorso pubblico era quello di evitare ogni possibile sospetto sul nuovo standard.

Cifratura a chiave simmetrica AES

- I requisiti richiesti erano:
  - utilizzo di crittografia a chiave simmetrica;
  - progetto completamente pubblico;
  - chiavi di lunghezza 128, 192 e 256 bit;
  - implementazione hw e sw;
  - algoritmo doveva essere liberamente utilizzato o non avere restrizioni particolari.

AES - Rijndael

- L'algoritmo prescelto è stato il Rijndael (Rijmen e Daemen)
- la selezione si è basata su criteri di sicurezza, efficienza, semplicità, flessibilità e requisiti di memoria (per sistemi embedded).
- Supporto chiavi e blocchi di cifratura da 128 a 256 bit, a passi di 32 bit
- blocchi e chiavi possono avere diversa lunghezza.
- L'utilizzo più frequente prevede chiavi di 128 o 256 bit e blocchi di 128 bit.

Cifratura a chiave simmetrica

- Collocazione dei dispositivi di cifratura, due possibilità:
  - Sulle linee (il pacchetto rimane vulnerabile nei commutatori)
  - Sui dispositivi terminali (non è possibile cifrare anche le intestazioni ma solo i dati)
- L'ottimo e utilizzare ambedue i metodi.

Cifratura a chiave pubblica

- Utilizza due chiavi:
  - Una chiave K_A usata per la cifratura che viene resa pubblica (chiave pubblica).
  - Una chiave K_B usata per la decifratura che viene mantenuta segreta (chiave privata).
- Si evita (ma solo parzialmente!) il problema della distribuzione della chiave.
- Deve avere tre requisiti
  - $D_{KB}(E_{KA}(P)) = P$
  - Non deve essere possibile dedurre K_B da K_A.
  - K_B non deve poter essere dedotta tramite cifratura di testi noti

Cifratura a chiave pubblica
Rivest, Shamir, Adelson (RSA)

Scelta delle chiavi

- Si scelga due numeri primi grandi (ad esempio da 1024 bit): **p** e **q**.
- Si calcoli **n = p · q**, **z = (p -1)(q -1)**.
- Si scelga **e** (con **e < n**) tale che non abbia fattori comuni con **z** (**e** e **z** sono “primi relativi”) **.**
- Si scelga **d** tale che **ed-1** sia esattamente divisibile per z (in altre parole **e · d mod z = 1.**
- La chiave pubblica K_A **= (n, e)** e la chiave privata K_B **= (n, d).**

Cifratura a chiave pubblica
Rivest, Shamir, Adelson (RSA)

- Dati (**n**, **e**) e (**n**, **d**):
  - Per cifrare una sequenza di bit **m**, si calcola:

    $\mathbf{c = m^e \bmod n}$ (ossia il resto di $\mathbf{m^e}$ diviso **n**)
  - Per decifrare una sequenza di bit **c** ricevuta, si calcola:

    $\mathbf{m = c^d \bmod n}$ (ossia il resto di $\mathbf{c^d}$ diviso **n**)
- Ciò che accade è che

$$\mathbf{m = (m^e \bmod n)^d \bmod n}$$

Cifratura a chiave pubblica
Rivest, Shamir, Adelson (RSA)

Bob sceglie **p** = 5, **q** = 7.

Quindi **n** = 35, **z** = 24.

e = 5 (così **e**, **z** sono primi relativi).

d = 29 (così **ed-1** è divisibile esattamente per **z**).

Cifra:

Lettera	m	m^e	$c = m^e \bmod n$
l	12	248832	17

Decifra:

c	c^d	$m = c^d \bmod n$	Lettera
17	48196857210675091509141182522307200 0	12	l

Cifratura a chiave pubblica
Rivest, Shamir, Adelson (RSA)

- Perché vale $m = (m^e \bmod n)^d \bmod n$?
- La base è un risultato della teoria dei numeri, ossia se p e q sono primi e n = p q allora:

$$x \bmod n = x^{e \bmod (p-1)(q-1)} \bmod n$$

- $(m^e \bmod n)^d \bmod n = m^{ed} \bmod n =$

$= m^{ed \bmod (p-1)(q-1)} \bmod n =$

(grazie al risultato della teoria dei numeri di cui sopra)

$= m^1 \bmod n =$

(dato che si è scelto **ed** divisibile per **(p-1)(q-1)** con resto 1)

$= m$

Cifratura a chiave pubblica
Rivest, Shamir, Adelson (RSA)

- Si osservi che l'algoritmo funziona anche a chiavi invertite.
- Il meccanismo è sicuro perché, al momento, non sono noti algoritmi veloci per la fattorizzazione dei numeri (altrimenti basterebbe fattorizzare n)
- Il problema della cifratura a chiave pubblica è il tempo di elaborazione, rispetto alla chiave simmetrica:
  - In software è 100 volte più lenta
  - In hardware è da 1000 a 10.000 volte più lenta
- Allora viene usato, in genere, solo per lo scambio di una chiave simmetrica di sessione.

Integrità e firma elettronica

- La firma elettronica è la forma più completa di verifica di integrità. Tale tipo di firma dovrebbe far sì che:
  - L'integrità del messaggio originale sia assicurata.
  - La firma sia legata indissolubilmente al messaggio.
  - La firma sia verificabile (permette di identificare chi ha firmato).
  - La firma sia non falsificabile e non rifiutabile (solo quell'individuo deve poter fare quella firma e non deve poterla disconoscere).

Firma elettronica

- Un modo per firmare il proprio documento è quello di codificarlo con la propria chiave privata.
- Dato che solo il proprietario ha la chiave privata, questo assicura che solo lui può averlo codificato, e chiunque può verificare che è stato lui a codificarlo usando la sua chiave pubblica e ritrovando il messaggio.
- Questo procedimento ha un limite:
  - La cifratura di un messaggio (con chiave pubblica) è una operazione onerosa se fatta su grandi quantità di dati. E lo stesso vale per la decifratura, obbligatoria per poter leggere il messaggio

Firma elettronica

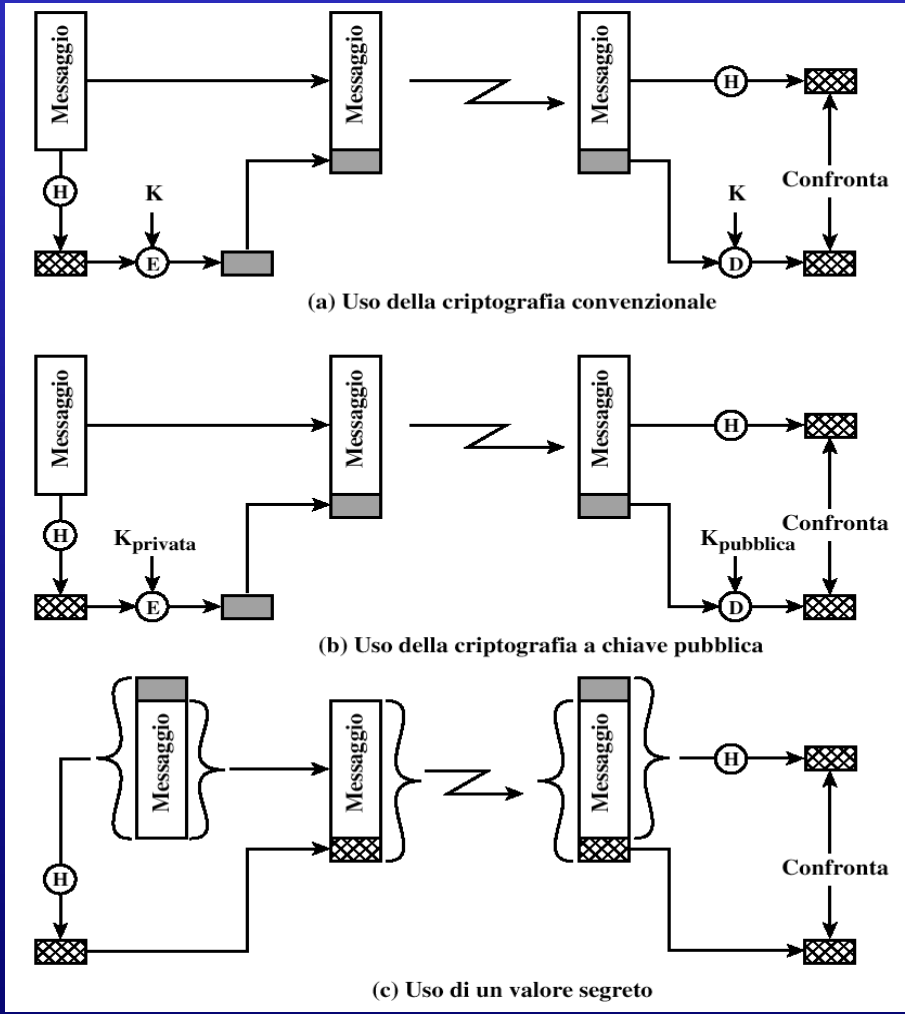
- Un meccanismo alternativo che impone un minor onere computazionale è quello del ***message digest*** (sunto del messaggio).
- Il principio è simile a quello dei codici a rivelazione d'errore, si applica ad un messaggio p una funzione H( ) il cui risultato è un blocco di dati d_p (il ***digest***) con dimensioni molto minori di p. Tale *digest* deve essere legato in modo univoco la messaggio originale
- Tale funzione H() viene chiamata funzione di **hash** .

Integrità e Firma elettronica
Digest

- La funzione di ***hash*** H() deve avere le seguenti proprietà:
  - Deve poter essere applicata a messaggi di qualunque dimensione.
  - Deve produrre un risultato di lunghezza fissa
  - Deve essere relativamente semplice da calcolare.
  - Per ogni *digest* d dato, deve essere computazionalmente impossibile trovare x tale che H(x) = d (non invertibilità).
  - Per ogni messaggio x deve essere computazionalmente impossibile trovare y ≠ x tale che H(y) = H(x) (impedisce falsificazioni).
  - Deve essere computazionalmente impossibile trovare una qualsiasi coppia (x, y) tale H(x) = H(y).

Integrità e Firma elettronica: Digest

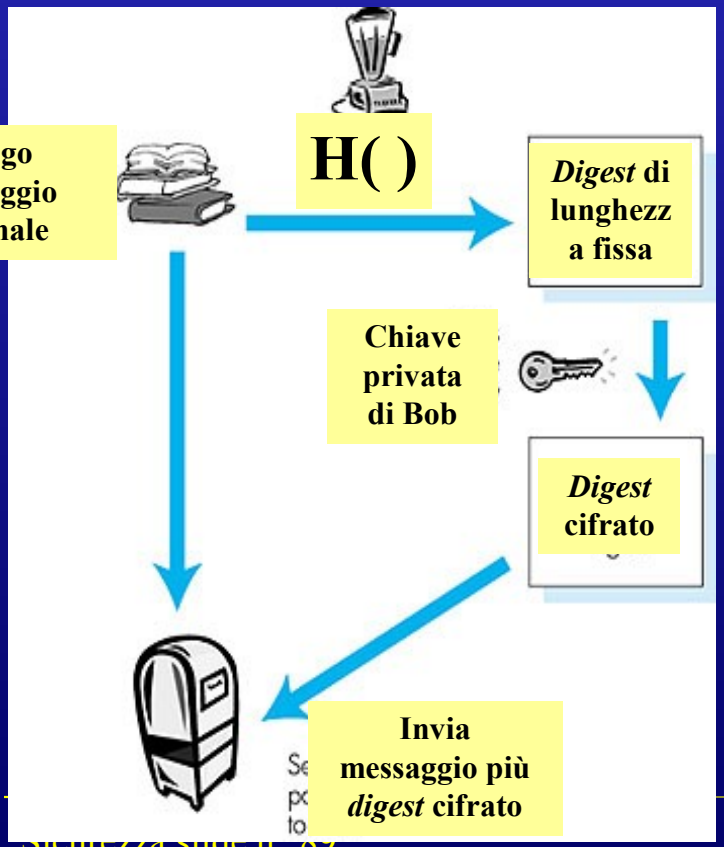
Possibili usi del *digest* per la verifica dell'integrità



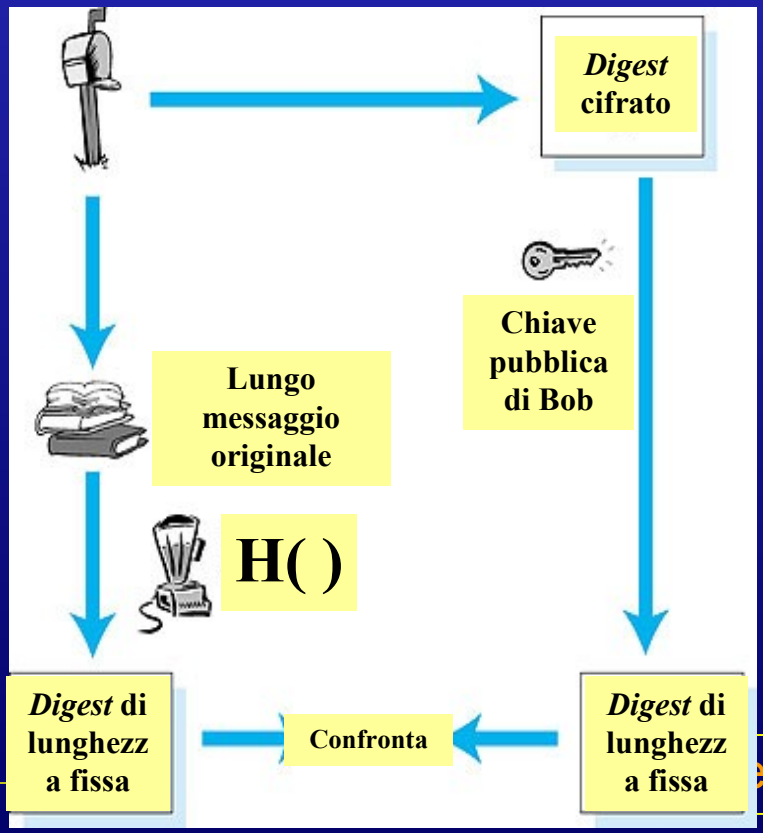
Integrità e Firma elettronica
Digest

- Si può usare il *digest* cifrato con la chiave privata corrisponde a firmare il messaggio

Bob "firma" ed invia



Alice riceve e verifica la firma



Integrità e Firma elettronica
Digest

- Gli standard più usati per il *digest* attualmente sono sostanzialmente due:
  - ***Secure Hash Algorithm*** (**SHA**): sviluppato dal NIST e rivisto successivamente e standardizzato come FIPS PUB 180-1 noto come **SHA-1**, e usa *digest* da 160 bit.
  - MD5 definito da Ron Rivest [RFC 1321] che usa un *digest* di 128 bit.

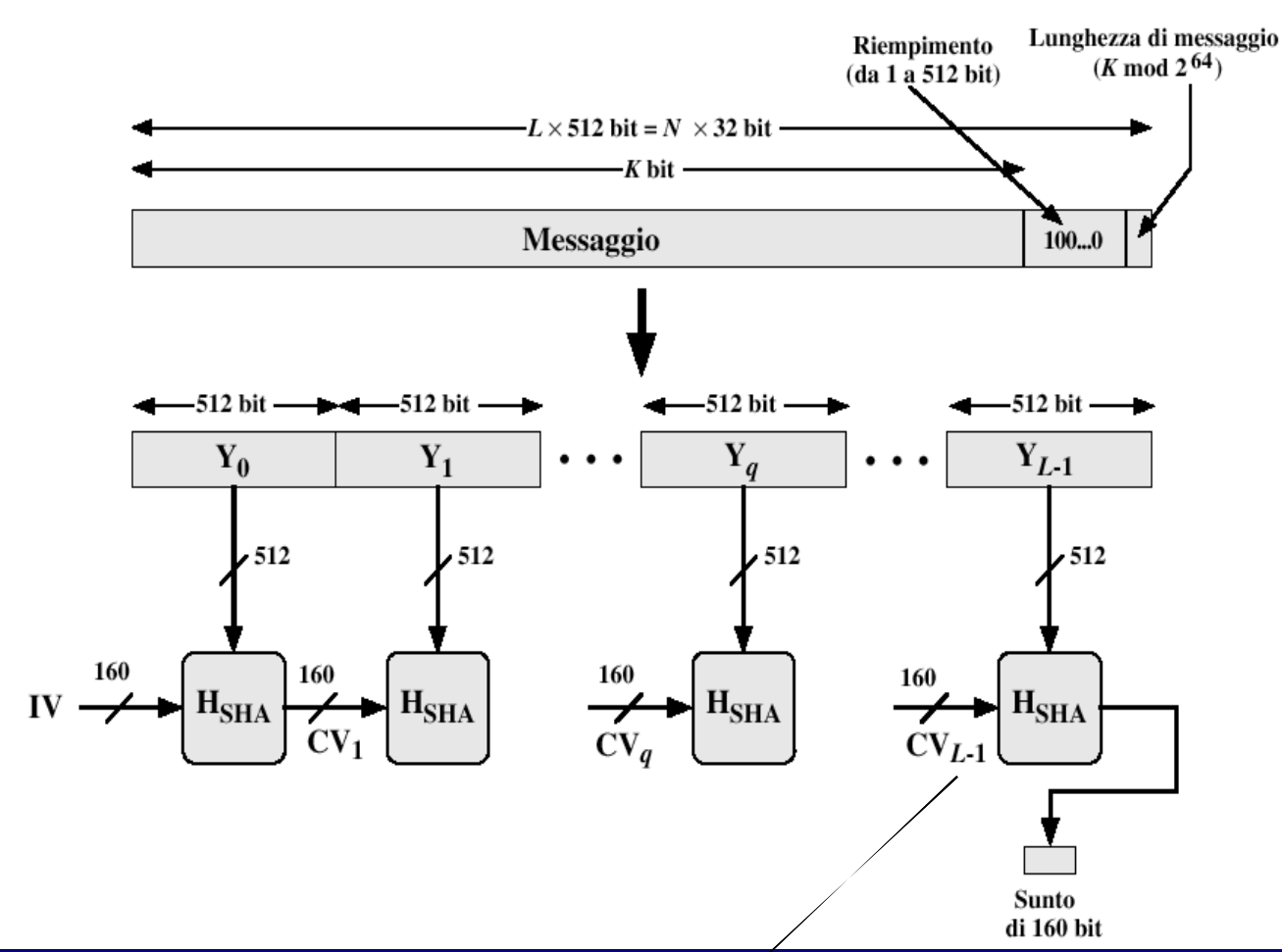
Integrità e Firma elettronica

Digest - MD5

N x 512 bit

N x 512 - 64

Integrità e Firma elettronica
Digest - SHA-1



Composto da 4 cicli da 20 passi

Ph.D. Carlo Nobile

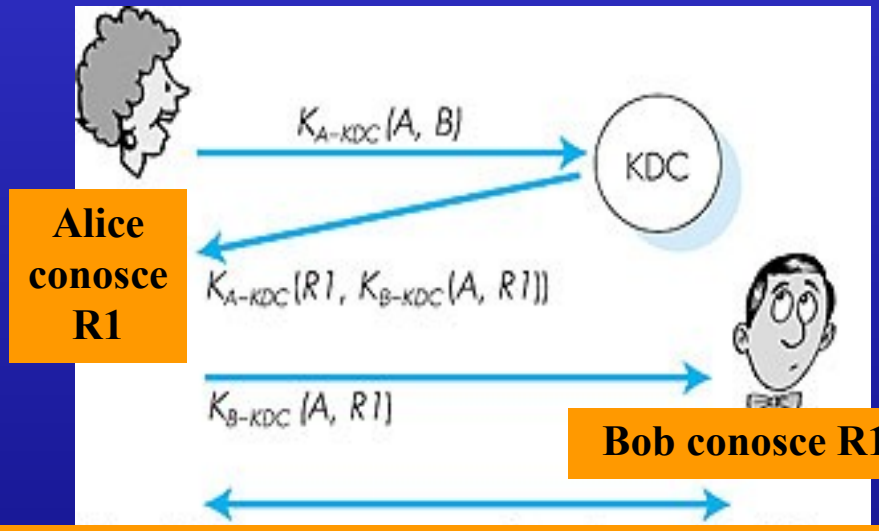
Distribuzione delle chiavi e certificazione

- Due entità che voglio comunicare cifrando con chiave simmetrica, come stabiliscono una chiave segreta comune?
- La soluzione è un centro di fiducia che distribuisca le chiavi (***Key Distribution Center***, **KDC**).
- Per la chiave pubblica-privata, il problema è un altro: come si fa ad essere sicuri della "proprietà" di una chiave pubblica?
- Anche in questo caso bisogna avere un intermediario di fiducia detto Autorità di certificazione (***Certification Authority***, **CA**) che certifichi l'appartenenza di una chiave pubblica.

Distribuzione delle chiavi e certificazione

Key Distibution Center

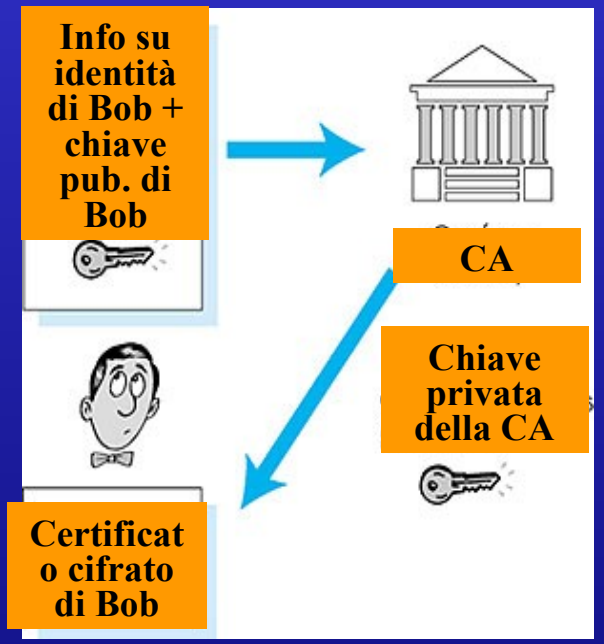
- Alice e Bob hanno bisogno di una chiave simmetrica comune.
- **KDC**: un server condivide una chiave segreta con ciascuno degli utenti registrati.
- Alice, Bob conoscono la propria chiave simmetrica, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, per comunicare con il KDC.



- Alice comunica con il KDC, acquisisce la chiave di sessione R1, e $K_{B\text{-}KDC}(A,R1)$
- Alice invia a Bob $K_{B\text{-}KDC}(A,R1)$ e Bob estrae R1
- Alice e Bob ora condividono la chiave simmetrica R1.

Distribuzione delle chiavi e certificazione
Certification Authority (CA)

- La ***Certification Authority*** (**CA**) lega una chiave pubblica ad una entità.
- Le entità (persone, router, etc.) possono registrare le loro chiavi pubblica alla CA.
  - L'entità che si iscrive deve fornire una "prova dell'identità" alla CA.
  - La CA crea un **Certificato** che lega l'entità alla chiave pubblica.
  - Il certificato viene "firmato" dalla CA.



- Quando Alice vuole la chiave pubblica di Bob:
- Prende il certificato di Bob (da Bob, dalla CA o ovunque).
- Applica la chiave pubblica del CA e ricava la chiave pubblica di Bob.

Distribuzione delle chiavi e certificazione

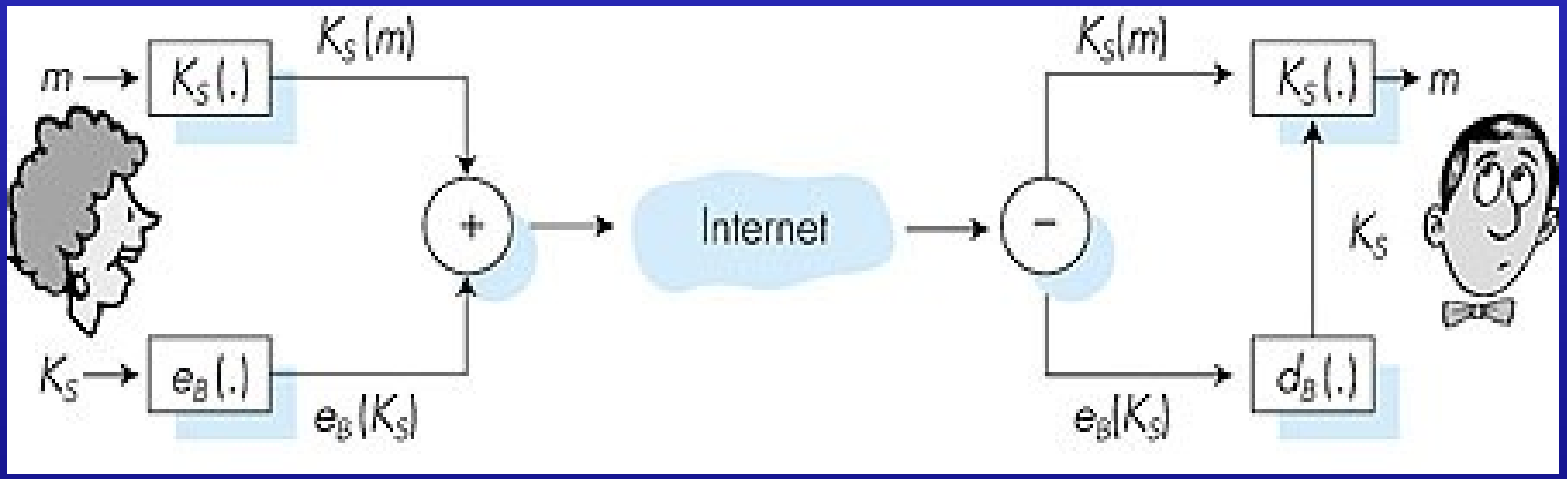
- Si osservi che la pratica usuale è quella di:
  - Usare chiave simmetriche per la cifratura dei dati (più veloci).
  - Cambiare spesso (ogni sessione o più) la chiave simmetrica.
  - Scambiarsi la chiave simmetrica tramite una cifratura a chiave pubblica.
  - Autenticare l'identità della chiave pubblica usando una CA.

Sicurezza - Protocolli

- Oltre che dal punto di vista della locazione fisica dei meccanismi di sicurezza, riveste una notevole importanza la scelta del loro posizionamento nella pila protocollare.
- I dispositivi di sicurezza possono essere implementati:
  - A livello di applicazione (ad es. email-PGP)
  - A livello di trasporto (ad es. SSL, SET)
  - A livello di rete (IPsec)
  - A livello di linea (WLAN)

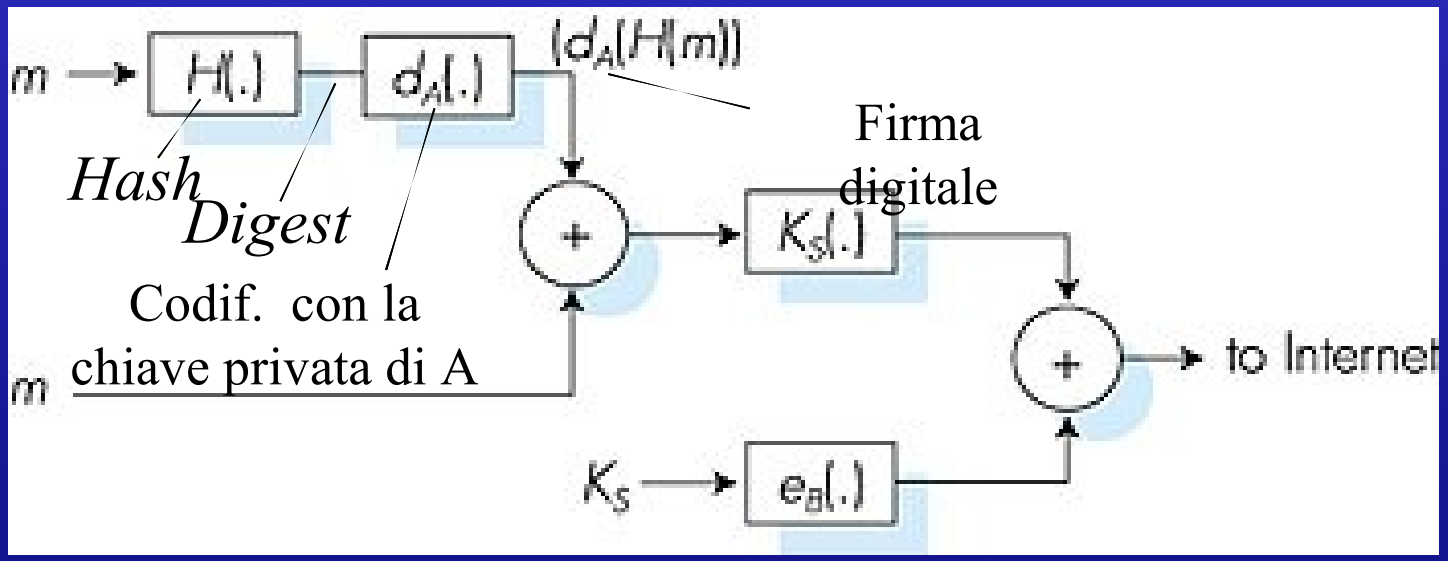
E-mail sicure - Segretezza dei dati

- Alice vuole inviare un messaggio m segreto a Bob



- Genera una chiave simmetrica casuale , K_S
- Cifra il messaggio con K_S, $K_S(m)$.
- Cifra anche K_S con la chiave pubblica di Bob, $e_B(K_S)$.
- Invia sia $K_S(m)$ che $e_B(K_S)$ a Bob

E-mail sicura - Segretezza, autenticazione ed integrità



- Il digest del messaggio viene cifrato con la chiave privata del mittente (firma e integrità)
- Il messaggio viene cifrato con una chiave simmetrica insieme alla firma; il tutto viene cifrato con la chiave pubblica del destinatario (segretezza)

E-mail sicura - PGP

Pretty Good Privacy (PGP)

- E' uno schema di di cifratura per e-mail, uno standard de facto.
- Usa la cifratura simmetrica (Triple-DES o IDEA) e a chiave pubblica (RSA), le funzioni di *Hash* (MD5 o SHA) e la firma digitale come descritto prima
- Quindi fornisce riservatezza, autenticazione del mittente e verifica dell'integrità del messaggio
- Inventato da Phil Zimmerman, oggetto per tre anni di indagini da parte federale (USA).

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3m
   qJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Ph.D. Carlo Nobile

Secure Socket Layer (SSL)

- SSL opera a livello di trasporto e fornisce funzioni per la sicurezza ad ogni applicazione basata su TCP
- E' utilizzato da varie applicazioni fra cui www *server* e *browser* per servizi di *e-commerce* (shttp)
- I servizi per la sicurezza di SSL sono:
  - Autenticazione del server (tramite certificato firmato da CA fidate)
  - Cifratura dei dati
  - Autenticazione dei client (opzionale)
- E' la base della ***Transport Layer Security (TSL)*** dell'IETF

Secure Socket Layer (SSL)

Autenticazione del server

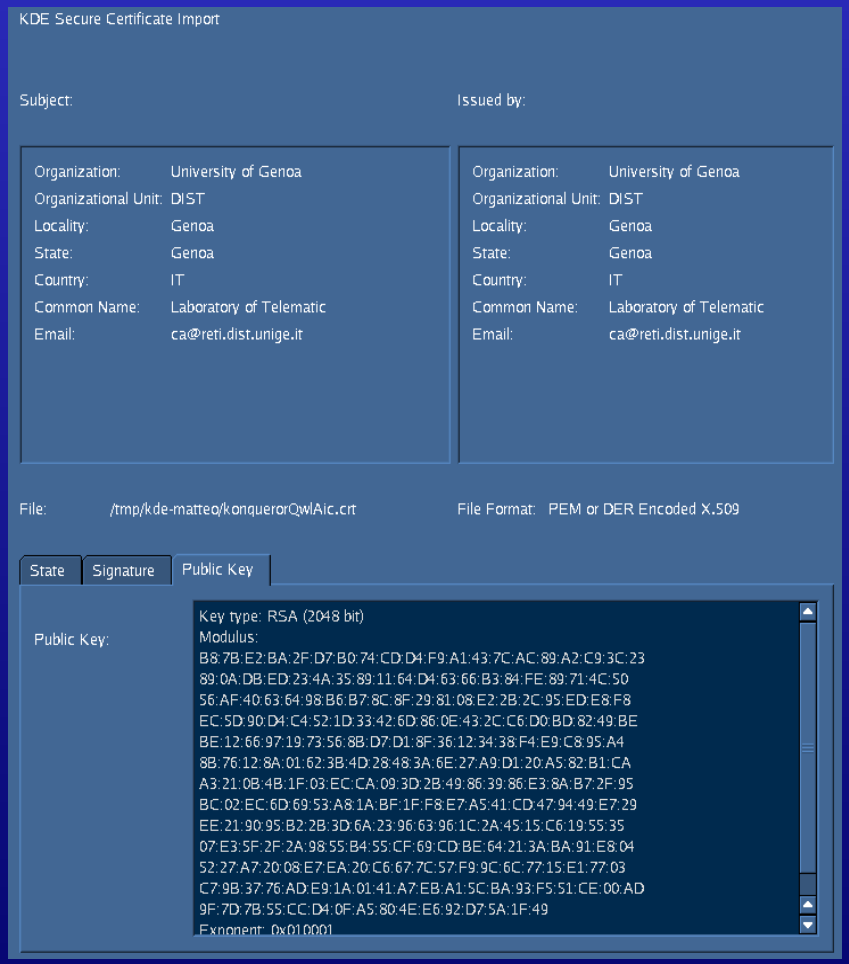
- Un *browser* con SSL deve possedere la chiave pubblica di una o più CA.
- Il *browser* richiede il certificato del Server secondo uno dei CA che conosce.
- Il *browser* usa la chiave pubblica del CA per estrarre la chiave pubblica del Server.

Sessioni SSL

- Per effettuare lo scambio sicuro, SSL crea delle sessioni che possono essere usate anche da più connessioni TCP contemporaneamente
- La sessione prevede:
  - la generazione di una chiave simmetrica da parte del *browser*, cifrata con la chiave pubblica del server e ad esso inviata;
  - La decifratura della chiave simmetrica da parte del server
  - Uno scambio per definire se e come i messaggi verranno cifrati

Distribuzione delle chiavi e certificazione

Certificati

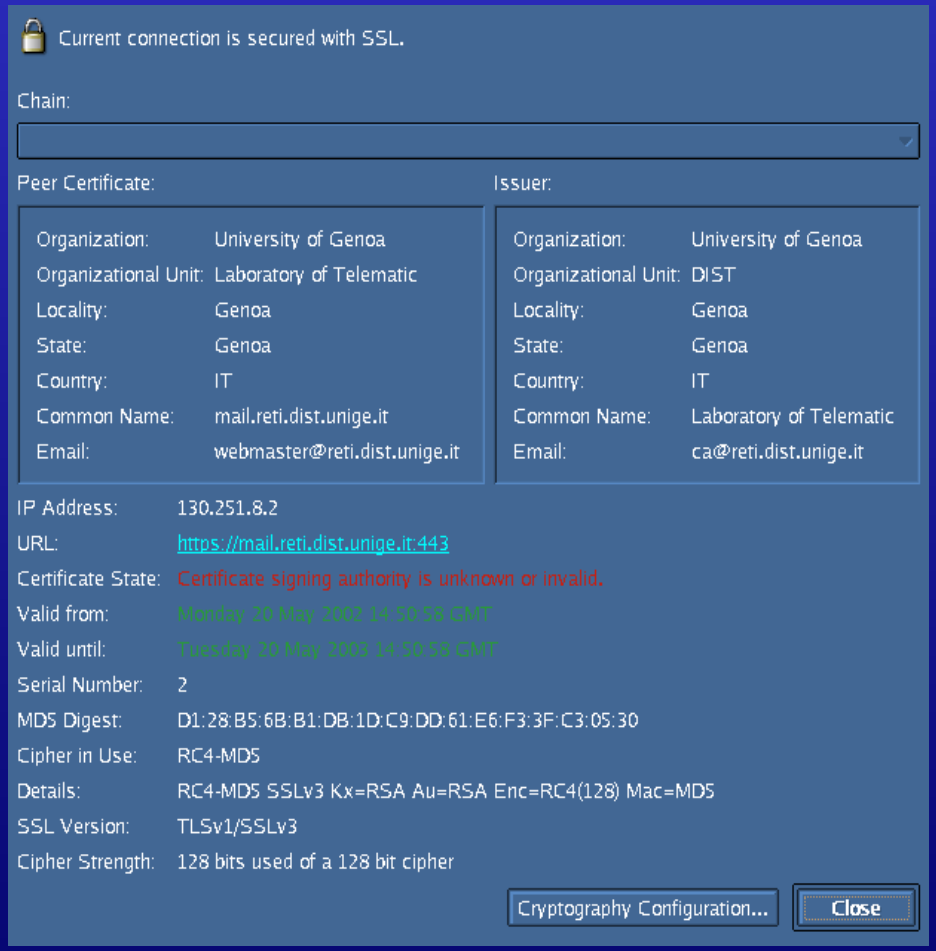


Certificato di una CA autofirmato

Ph.D. Carlo Nobile

Distribuzione delle chiavi e certificazione

Certificati

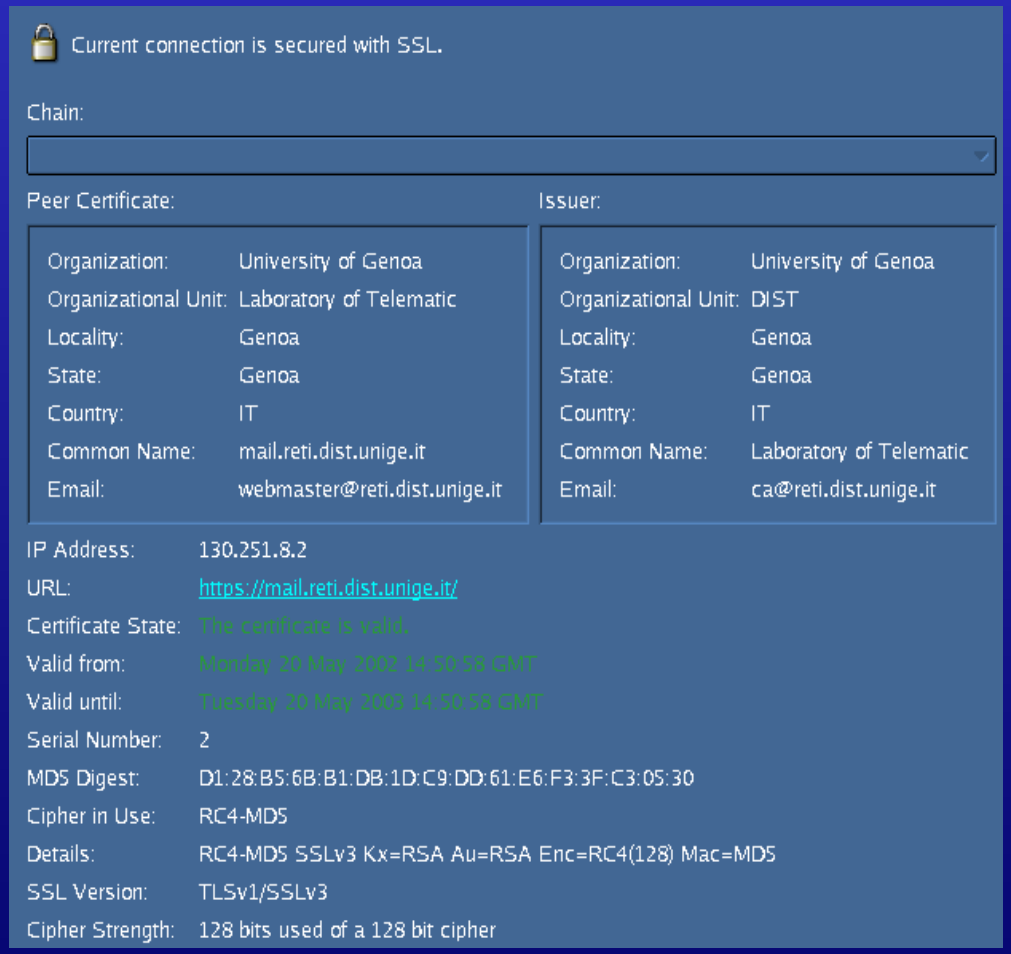


Certificato di un server web firmato da una CA non riconosciuta dal browser

Ph.D. Carlo Nobile

Distribuzione delle chiavi e certificazione

Certificati



Certificato di un server web firmato da una CA riconosciuta dal browser

Ph.D. Carlo Nobile

Secure Electronic Transaction (SET)

- E' stato progettato per realizzare i pagamenti via carta di credito e le transazioni via Internet (VISA e Mastercard);
- Prevede la presenza di tre attori che devono essere tutti certificati:
  - Cliente (certificato dalla propria banca)
  - Venditore (certificato dalla propria banca)
  - Banca (del venditore)
- Dà significato legale ai certificati;
- Il numero di carta di credito del cliente passa alla banca del venditore senza che quest'ultimo lo possa vedere.
- Tre componenti software:
  - *Browser wallet* (portafoglio)
  - *Merchant server*
  - *Acquirer Gateway*

Sicurezza a livello di rete
IPsec (IP security)

- La cifratura continua ad essere *end-to-end* ma viene effettuata nel livello di rete sui pacchetti IP e quindi diventa disponibile a tutti i protocolli che usano IP (oltre TCP, UDP, ICMP, SNMP,…).
- Per quanto concerne l'autenticazione, in questo caso questa può avvenire anche nei confronti di indirizzi IP.
- IPsec si compone di due protocolli:
  - ***Authentication Header* (AH) *protocol***
  - ***Encapsulation Security Payload* (ESP) *protocol***

Sicurezza a livello di rete
IPsec (IP security)

- Alcuni esempi di utilizzo di IPsec sono:
  - Interconnessione sicura di reti aziendali tramite Internet (in sostanza permette la realizzazione di ***Virtual Private Network*** (VPN)).
  - Accesso remoto sicuro in Internet.
  - Interconnessione sicura fra organizzazioni diverse via Internet.
  - Migliore sicurezza nel commercio elettronico.

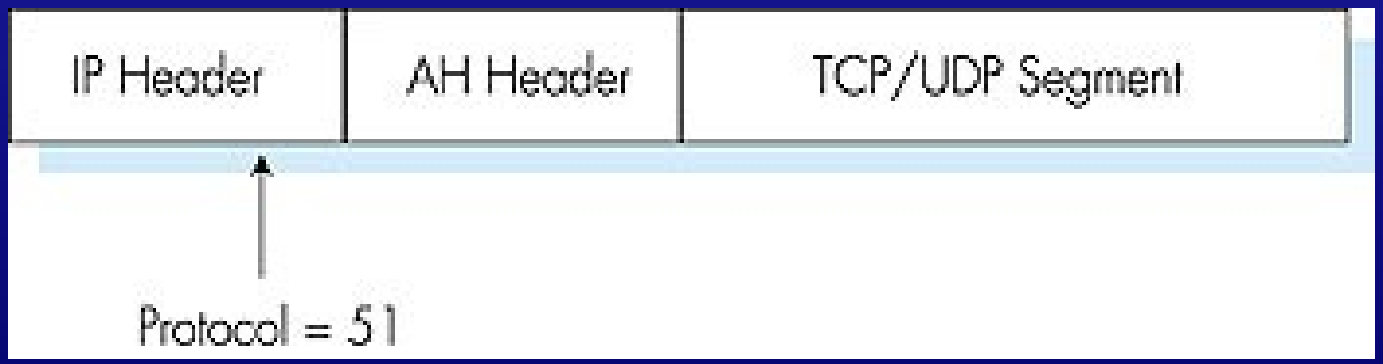
Sicurezza a livello di rete
IPsec (IP security)

- Ambedue i protocolli di IPsec (ESP e AH) operano tramite una canale logico a livello di rete chiamato ***Security Association*** (**SA**), creato tra sorgente e destinazione con un *handshake*.
- L'SA è
  - Unidirezionale
  - Univocamente determinato da:
    - Protocollo di sicurezza usato (ESP o AH).
    - Indirizzo IP della sorgente.
    - ID a 32 bit della connessione (SPI, *Security Parameter Index*).

Sicurezza a livello di rete
IPsec - AH

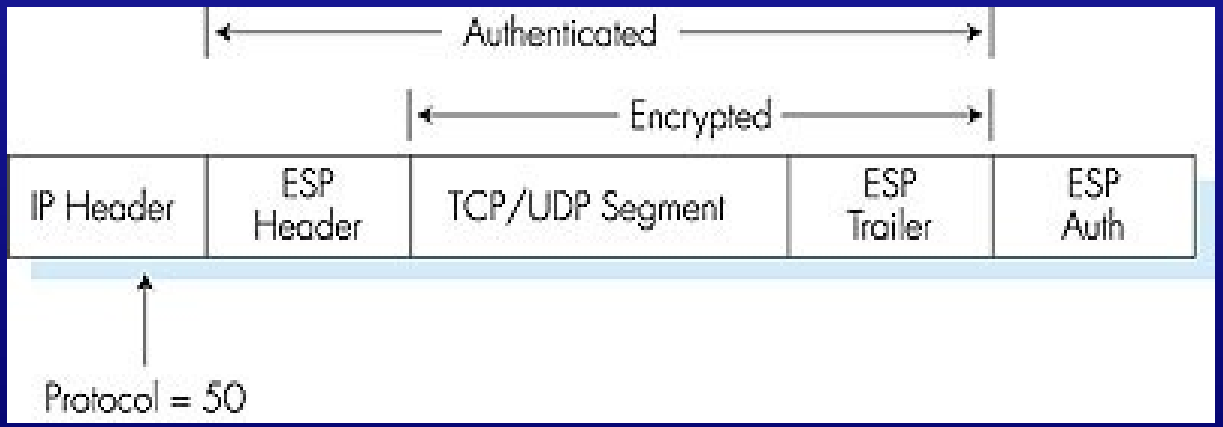
- Fornisce l'autenticazione dell'*host* e l'integrità dei dati ma non la riservatezza.
- L'intestazione AH viene inserita fra quella IP ed i dati
- Il numero di protocollo è il 51
- I *router* intermedi elaborano il *datagram* in modo usuale.

- L'intestazione dell'AH comprende:
  - Un identificatore di connessione
  - Un *digest* "firmato"e calcolato sul *datagram* originale
  - Un campo che specifica il tipo di dati trasportati (UDP, TCP, ICMP…)
  - Un numero di sequenza



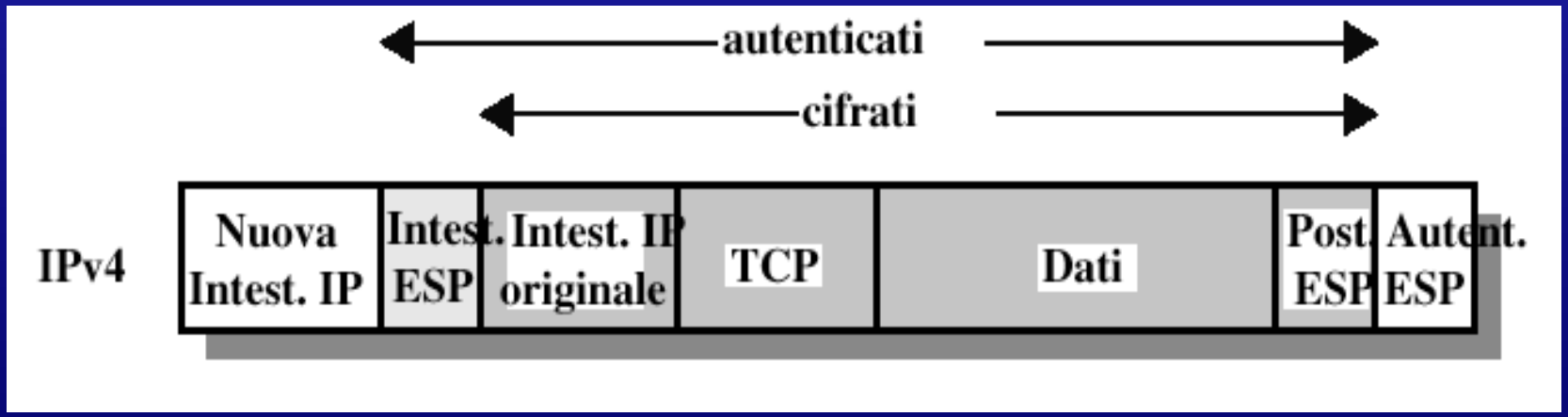
Sicurezza a livello di rete
IPsec - ESP

- Fornisce la riservatezza, l'autenticazione dell'host e l'integrità dei dati
- I dati e il postambolo dell'ESP sono cifrati
- L'indicazione della successiva intestazione è nel postambolo ESP.
- Il campo di autenticazione del ESP è simile ha quello dell'AH
- Il numero di protocollo contenuto nell'intestazione IP quando si usa ESP è 50



Sicurezza a livello di rete
IPsec - Modalità di trasporto

- Due sono le modalità di funzionamento:
  - Modalità di trasporto
  - Modalità Tunnel
    - applicabile se le due entità sono apparati intermedi come *router*.
    - permette comunicazioni sicure a terminali che non usano IPsec.
    - Permette la cifratura dell'intero pacchetto IP.



Sicurezza a livello di rete
IPsec - SA

- Per il funzionamento di IPSec é necessario un meccanismo automatico per lo scambio e la gestione delle chiavi
  - *Internet Key Exchange* (IKE, RFC 2409) é il protocollo di default per lo scambio delle chiavi dell'IPSec
  - *Internet Security Association and Key Management Protocol* (ISKMP, RFC 2047 e 2048) definisce le procedure per stabilire ed interrompere gli SA. L'associazione per la sicurezza ISKMP é completamente separata dallo scambio di chiavi IKE.